Slovenská Technická Univerzita v Bratislave

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Návrh manažmentu pre dohľad nad sieťou Ústavu telekomunikácií

Referát

2012 **Bc. et Bc. Andrej Ralbovský**

Zadanie

1. **Navrhnite manažment pre dohľad nad sieťou na ÚT FEI STU v Bratislave**
2. Vypracujte referát, v ktorom svoj návrh popíšete.
3. Pripravte si krátku prezentáciu (cca. 7 minút), počas ktorej svoj návrh odprezentujete.

Obsah

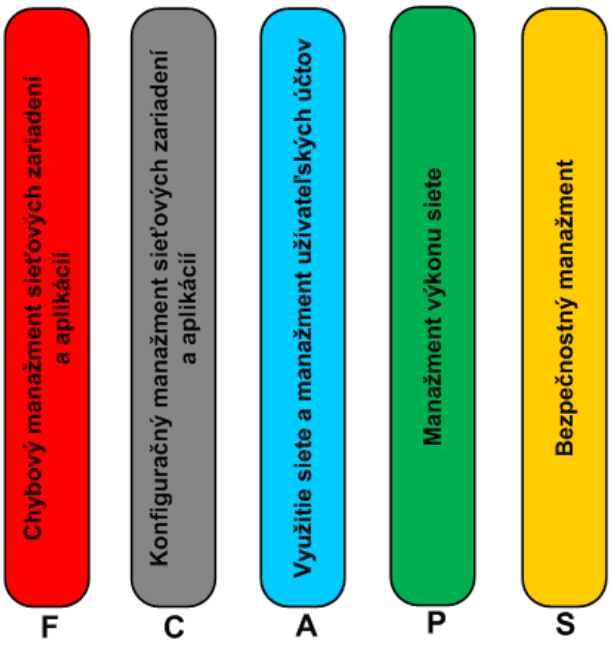
Úvod

Každá väčšia sieť, najmä však v korporátnom prostredí, vyžaduje systematizovaný prístup k svojmu riadeniu. Kým pri sieťach menších rozmerov (rádovo jednotky pracovných staníc, žiadne zložité konfigurácie prepojení, servery umiestnené mimo uvažovanej siete) môže byť riadenie siete a dohľad nad ňou realizované priamo fyzickými zásahmi správcu na jednotlivých zariadeniach a neformálnymi procesmi, siete väčších rozmerov, medzi ktoré môžeme zaradiť aj sieť Ústavu telekomunikácií (ďalej len ÚT, prípadne Ústav) je potrebné riadiť s využitím špecializovaného programového vybavenia, ktoré manažment výrazne uľahčuje a správcovi dáva mnoho viac možností realizovať svoje úlohy pri súčasnom zvýšení svojej efektivity a optimalizácií využitia prostriedkov siete, ako aj zvýšení bezpečnosti.

V tejto práci opisujeme topológiu siete, analyzujeme požiadavky kladené na takýto systém riadenia a uvádzame dve navrhované alternatívy, ktoré sa líšia v použitom softwari (Cacti vs.Zabbix) a komplexnosti jeho údržby a inštalácie, ale aj v možnostiach, ktoré sú správcovi siete poskytované.

1. FCAPS model

Vypracovaný návrh manažmentu siete je podľa funkčného modelu FCAPS [1] (Fault, Configuration, Accounting, Performance, Security), ktorý je definovaný ako štandard podľa ISO aj ITU.



Obr. 1: Model FCAPS

Nie sú však zahrnuté úplne všetky jeho kategórie, nakoľko sieť ÚT je špecifická, čo sa týka účelu využívania. Taktiež sú využité možnosti súčasného stavu, keď sú všetky používateľské účty, údaje a profily centrálne uložené a spravované na unixovom serveri.

2. Požiadavky

Pri návrhu manažmentu sme vychádzali z toho, že je potrebné splniť nasledujúce požiadavky:

1. Minimalizácia nákladov – nakoľko Ústav telekomunikácií je vysokoškolským pracoviskom a slovenské vysoké školstvo je finančne poddimenzované, zachovanie čo najnižších nákladov je jednou zo základných požiadaviek. Musí byť kladený dôraz na čo najnižšiu cenu jednotlivých častí manažmentového systému, teda tak hardwaru, ako aj softwaru a osobných nákladov na pracovníkov zabezpečujúcich manažment siete, ale aj systému ako celku. V optimálnom prípade by obstarávacie náklady programového mali byť nulové, ak by bol použitý výlučne software pod Open Source licenciou.
2. Nezávislosť od dodávateľa – keďže Slovenská Technická Univerzita v Bratislave je verejnoprávnou inštitúciou, je potrebné prihliadať aj na spôsob obstarávania aktív. Ak náklady prekročia určitú hodnotu, musí sa konať formálne verejné obstarávanie podľa zákona, ktoré je náročné z hľadiska času aj administratívneho zaťaženia. Okrem toho je nutné myslieť aj na rozšíriteľnosť v budúcnosti a podľa toho vhodne pripraviť už súčasné riešenie, aby sa zabránilo vzniku situácie, že by bolo možné obstarať riešenie iba od jedného dodávateľa, alebo že by boli potrebné neúmerne veľké investície do prípadnej zmeny celého systému.
3. Jednoduchosť a strmá krivka učenia – ÚT má obmedzené kapacity pracovníkov údržby a obsluhy, nakoľko prevažná časť zdrojov je alokovaná na pedagogickú a výskumnú činnosť; aktuálne je na správu IT infraštruktúry jeden pracovník, aj to nie na plný úväzok; preto je nevyhnutné, aby bol jeho pracovný čas využitý čo najefektívnejšie, v prevažnej miere na činnosti vyplývajúce z jeho pracovnej náplne, nie na vzdelávanie, ktoré nie je nevyhnutné, aj keď v strednodobom časovom horizonte by mohlo znamenať určitý prínos
4. Nízka záťaž systémových prostriedkov – súvisí s požiadavkou minimalizácie nákladov; ÚT si nemôže dovoliť vydržovať samostatné servery len na manažment siete; je odôvodnený predpoklad, že manažmentový software bude musieť byť prevádzkovaný na už existujúcich serveroch poskytujúcich aj iné služby ako napríklad web, zálohovanie, FTP, Samba a iné
5. Rozšíriteľnosť - konfigurácia siete sa môže meniť; Ústav vykonáva svoju činnosť vo veľmi nestabilných podmienkach vonkajšieho prostredia vyplývajúcich z dynamického vývoja politickej a ekonomickej situácie, demografických trendov a stavu vedecko-technického

poznania a tiež v nemenej nestabilných podmienkach vnútorného prostredia, najmä procesov rozhodovania v akademickej samospráve na úrovni univerzity a fakulty, rozdeľovania finančných prostriedkov a fluktuácie pracovníkov. Nie je možné v blízkej budúcnosti vylúčiť zlučovanie či rozdeľovanie Ústavu, ani odčleňovanie niektorých jeho činností (napríklad správy IT na úroveň celej fakulty); taktiež musí byť možné dodatočne implementovať funkcionalitu, či už v podobe študentských prác alebo vedecko-výskumných projektov)

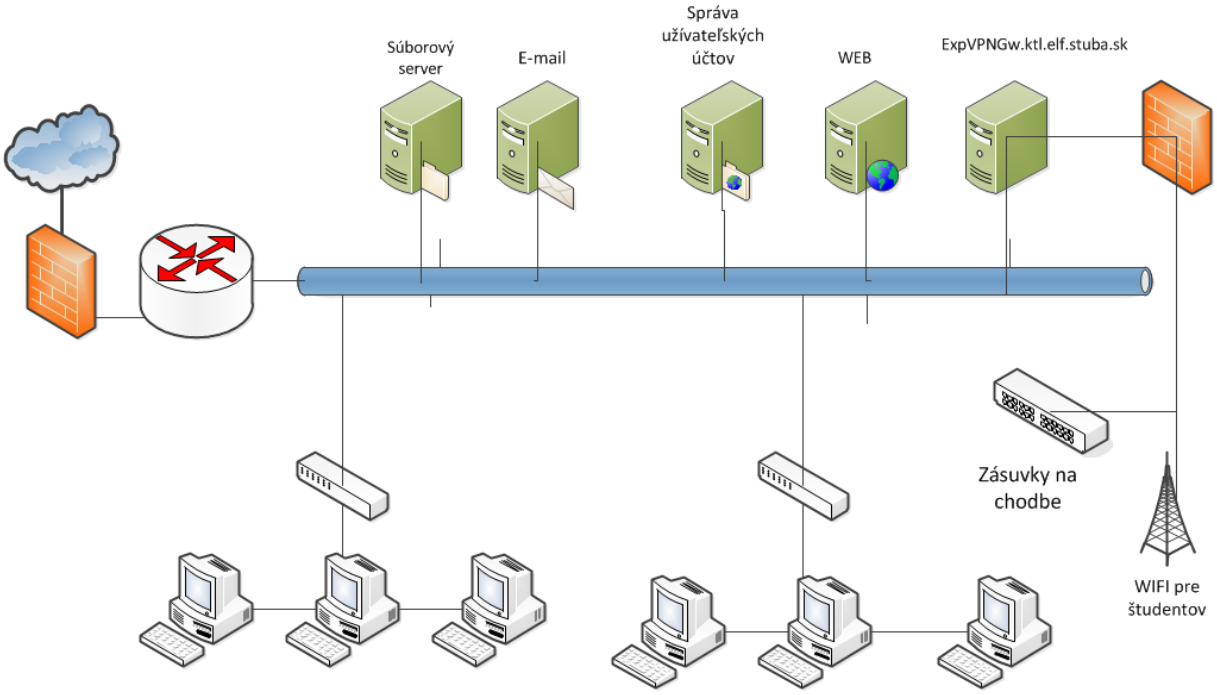
6. Škálovateľnosť – súvisí s predchádzajúcou požiadavkou; manažment musí byť možné rovnako efektívne vykonávať aj v prípade zväčšovania infraštruktúry Ústavu, pričom rast nákladov musí byť nanajvýš lineárny
7. Redundancia – odolnosť voči rôznym druhov výpadkov; táto požiadavka je protichodná s požiadavkou minimalizácie nákladov, nakoľko vyžaduje ďalšie hardwarové a sieťové prostriedky, avšak v prípade neočakávaných udalostí môže v konečnom dôsledku celkové náklady znížiť
8. Možnosť exportu vybraných údajov do externých systémov, prípadne prepojenia s monitorovacím systémom pre celú fakultu/univerzitu
9. Rýchla reakcia na incidenty – akékoľvek výpadky musia byť zistené a vyriešené čo najrýchlejšie, pretože môžu mať vplyv na produktivitu zamestnancov, najmä pokiaľ sa vyskytnú v pracovných hodinách
10. Poskytovanie relevantných informácií za určité časové obdobie – najmä dlhodobých štatistík, ktoré môžu byť použité pri plánovaní infraštruktúry do budúcnosti

3. Topológia siete Ústavu telekomunikácií

Ústav telekomunikácií má pridelené IP rozsahy [2] 147.175.103/24, 147.175.104/24 a 147.175.117.0/24. Prvý z nich je použitý pre zamestnaneckú časť siete, druhý pre študentskú. ÚT je pomerne malým pracoviskom, ktoré tvorí približne 30 zamestnancov a 23 doktorandov [3]. Organizačne sa delí na sekretariát a tri oddelenia – Oddelenie teórie oznamovacej elektrotechniky (OTOE), Oddelenie spojovacích systémov (OSS) a Oddelenie prenosových systémov (OPS). Pri našom návrhu budeme predpokladať, že tieto organizačné jednotky sú rovnocenné, čo do potrieb na jednotlivé časti IT infraštruktúry. Všetky sú na jednej IP podsieti 147.175.103.0/24 a poznať logické členenie nie je pre potreby hrubého návrhu manažmentu potrebné. Ústav poskytuje pripojenie do internetu (a cez VPN bránu aj do svojej siete) aj z respírií na 4., 5. a 6. poschodí bloku B, a to buď cez WIFI alebo ethernetové zásuvky. Na toto je vyhradená časť z neverejného rozsahu 192.168.0.0/24 a pri prístupe do internetu sú tieto IP adresy prekladané prostredníctvom NAT.

Sieť Ústavu telekomunikácií pozostáva niekoľkých desiatok pracovných staníc v kanceláriách zamestnancov a v učebniach a laboratóriách pre študentov, niekoľkých tlačiarní, IP kamier, IP telefónov, informačného kiosku na 4. poschodí, a niekoľkých serverov slúžiacich na zaistenie bežných sieťových služieb ako web Ústavu, elektronická pošta, ukladanie súborov, centrálne prihlasovanie a správa používateľských profilov. Tiež je tam niekoľko serverov slúžiacich na výskumné účely ako výskumné VoIP ústredne, cluster piatich serverov na hľadanie nových kódov nachádzajúci sa na 6. poschodí alebo IMS platforma od spoločnosti Alcatel, tieto však vzhľadom na špecifický účel používania a pretože neposkytujú služby nevyhnutné na činnosť Ústavu, nemusia byť spravované centrálne, a preto ich v našom návrhu nebudeme zohľadňovať.

Topológia siete ÚT je načrtnutá na obrázku.



Obr. 2: Topológia siete ÚT (schéma)

4. Aspekty návrhu spoločné pre obidve alternatívy

Aj keď sa jednotlivé alternatívy líšia v použitom manažmentovom softwari, ponúkaná funkcionalita je približne rovnaká, pri niektorých oblastiach je dokonca zhodná. Predovšetkým časť oblasti bezpečnostného manažmentu (správa používateľských účtov, prideľovanie oprávnení, kontrola prístupových práv, ...) a manažmentu konfigurácie (zálohovanie a obnovovanie, pravidelné spúšťanie úloh, automatizovaná distribúcia softwaru, ...) nie je súčasťou ani jedného z navrhovaných softwarových prostriedkov a je vyriešená na úrovni operačného systému (najmä unixové počítače) a centralizovanej správy používateľských účtov a profilov (s využitím softwaru Samba, ktorý je

nasadený na serveri v úlohe PDC (primary domain controller) a na ktorom je diskový priestor vyhradený pre súbory používateľov). Tomuto sa však v našom návrhu nebudeme venovať, nakoľko riešenie, ktoré už je v sieti implementované, je postačujúce. Pokiaľ ide o manažment účtovania, jeho funkcionalita je v sieti Ústavu telekomunikácií využívaná len minimálne, a to jednak z dôvodu pomerne nízkeho počtu užívateľov, ako aj pre charakter využívania služieb (používatelia nevyužívajú služby pre vlastné potreby, ale v prospech fakulty, resp. Ústavu, ktorý sieť na tento účel prevádzkuje). Jedným z mála druhov funkcionality tohto druhu môžu byť diskové kvóty. Tieto sú spravované, sledované a vynucované na serveri (resp. serveroch), kde je nasadený software Samba a kde sú uložené používateľské profily.

V prípade obidvoch alternatív nebude potrebné vyčleniť samostatný hardware na správu, aj keď použitá architektúra je manažér-agent. Manažmentové aplikácie je možné nainštalovať na už existujúce servery, pričom je možné spravovať aj tieto, na čo bude využitý lokálny SNMP agent. V zásade v celej sieti bude stačiť používať SNMP protokol, ale v prípade neštandardných zariadení alebo monitorovaných veličín je možné tieto obstarať s použitím skriptov. Prostredníctvom SNMP protokolu je možné zaistiť monitorovanie aj rôznych neštandardných veličín (napríklad systémové napätia, či údaje z lokálneho UPS pripojeného cez rozhranie USB alebo RS232), pokiaľ to agent podporuje. Pri serveroch s unixovým operačným systémom by to nemal byť problém, ak sa použije vhodný SNMP software, napríklad net-SNMP [4]. Na počítačoch s Microsoft Windows je taktiež možné použiť net-SNMP, namiesto štandardného SNMP agenta. V prípade zariadení s inými operačnými systémami to môže predstavovať isté ťažkosti. Bude potrebné vypísať vlastné skripty, ktoré budú tieto údaje získavať, napríklad prostredníctvom protokolu HTTP z webového rozhrania určeného pre správu.

Obidve riešenia, Cacti aj Zabbix ako používateľské rozhranie ponúkajú webové prostredie, teda nie je potrebné na počítači správcu inštalovať samostatný klientský software, nakoľko postačí internetový prehliadač.

Monitorované zariadenia a veličiny

Monitorované budú všetky zariadenia okrem vybraných pracovných staníc, u ktorých by to nemalo praktický význam. Monitorovať sa budú minimálne nasledujúce veličiny:

1. Záťaž
2. Využitie pamäte
3. Časy odoziev

→ výkonové veličiny

4. Dostupnosť
5. Uptime
6. Prenesené údaje

→ štatistické veličiny

7. Teplota okolia
8. Vlhkosť

→ veličiny prostredia

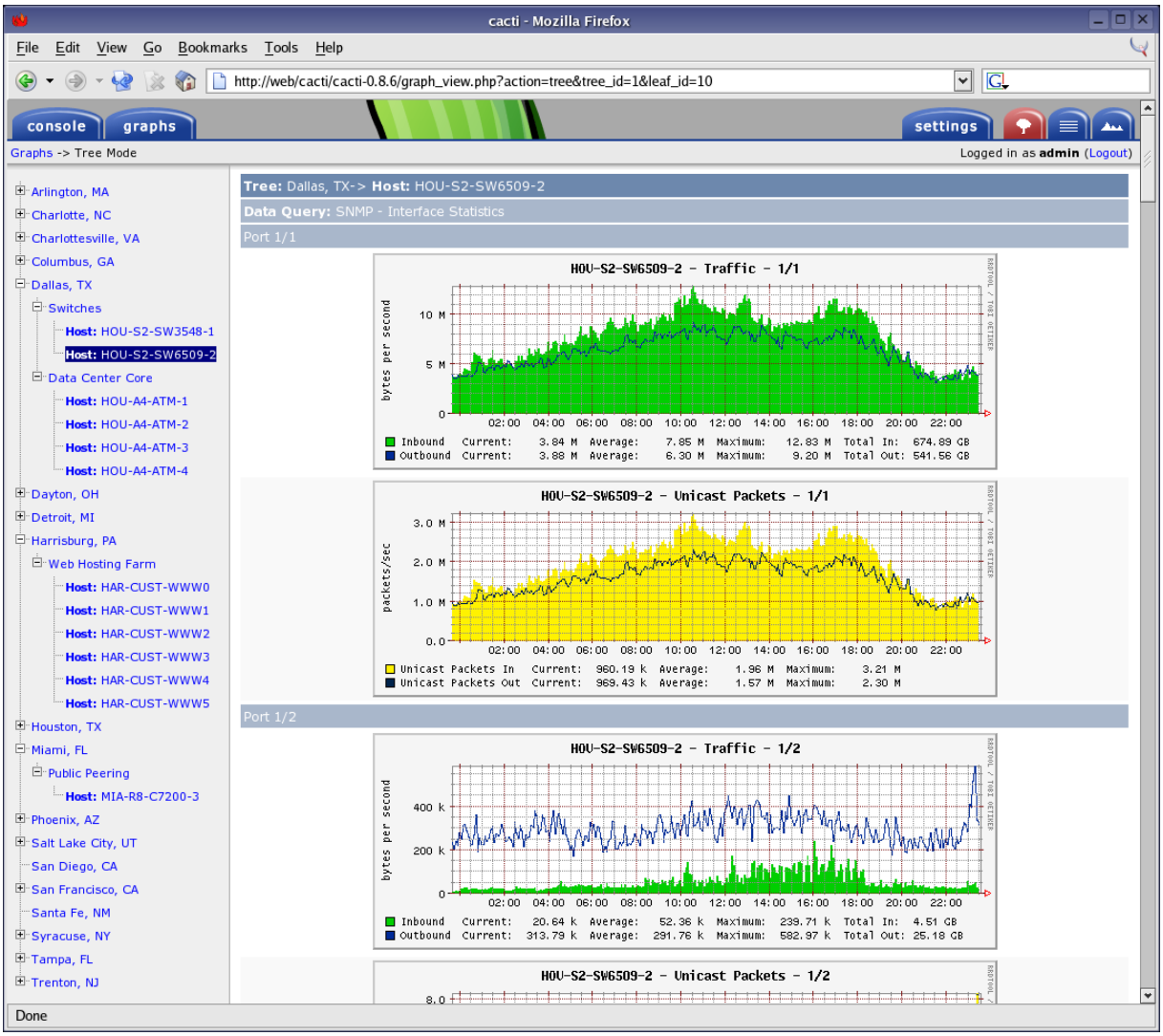
9. Otáčky ventilátorov
10. Systémové napätia
11. Systémové teploty
12. S.M.A.R.T údaje z pevných diskov

→ diagnostické veličiny

13. Údaje zo záložných zdrojov napájania

5. Alternatíva 1 – Cacti

Cacti je sada programov (PHP skriptov a démon na zbieranie údajov napísaný v jazyku C), ktorá bola pôvodne určená na jednoduché vykresľovanie grafov rôznych systémových veličín. Údaje z monitorovaných zariadení získava prostredníctvom protokolu SNMP alebo vlastnými skriptami napísanými pre špecifické účely. Získané údaje ukladá v MySQL [5] databáze. Na vytváranie grafov Cacti využíva nástroj RRDtool [6]. Pre naše potreby je však veľmi dôležité, že obsahuje možnosť využívania zásuvných modulov (plug-in) rozširujúcich funkcionalitu, takže okrem jednoduchého monitorovania (ktoré by zaisťovalo splnenie iba časti stanovených požiadaviek), môžeme prostredníctvom vhodných modulov realizovať aj zvyšné funkcionality zahŕňajúce ostatné aspekty manažmentu ako napríklad zasielanie upozornení na neočakávané udalosti (výpadok zariadenia, prekročenie prípustnej hodnoty veličiny, alarmy) a sledovanie trvania a odstraňovania poruchových stavov.



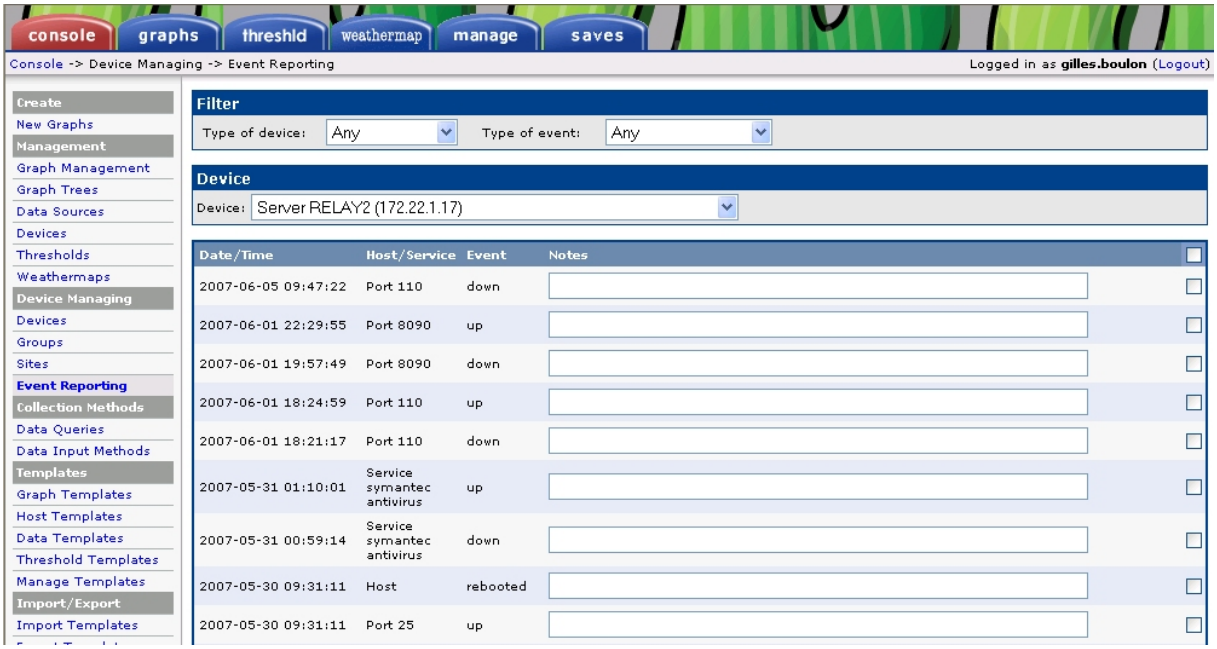
Obr. 3: Cacti

Preto okrem základnej inštalácie bude potrebné pridať nasledujúce moduly:

manage

Tento modul je určený na sledovanie stavu jednotlivých sieťových zariadení a ich riadenie. Je možné každému zariadeniu priradiť obrázok pre lepšiu orientáciu. Takisto je možné použiť konzolu na pripojenie k ľubovoľnému TCP portu (veľmi vhodné na účely ladenia, diagnostiky a testovania). Umožňuje tiež zvukové upozornenie alebo prostredníctvom emailu.

Obr. 4: Cacti s modulom na manažment



Obr. 5: Cacti - prehľad chybových udalostí

CaMM

Slúži na spracovávanie alarmov obdržaných prostredníctvom syslog démona alebo SNMP trap správ. V závislosti od definovaných pravidiel ich filtruje a ďalej spracováva, pričom z nich dokáže generovať upozornenia pre administrátora.

Thold

Umožňuje generovať chybové hlásenia pri výskyte hodnoty monitorovanej veličiny, ktorá je mimo prednastaveného povoleného rozsahu. Ponúka dobrú integráciu s ostatnými pluginmi pre Cacti.

Cacti je vhodným riešením pre menšie siete, ktoré nie sú spravované veľkým počtom administrátorov (čo platí aj pre sieť Ústavu). Má veľmi strmú krivku učenia a pomerne jednoducho sa nasadzuje. Taktiež je pomerne jednoduchá a časovo nenáročná aj jeho údržba. Miernou nevýhodou je, že pôvodne bol vyvíjaný iba ako nástroj na monitorovanie veličín, najmä však sieťových zariadení, ktorý mal zjednodušiť právu s RRDtool. Nemal teda pokrývať všetky druhy funkcionality sieťového manažmentu. Prostredníctvom zásuvných modulov sa to síce podarilo, no stále to nie je ucelená aplikácia, kde by administrátor dokázal všetko pohodlne vybaviť. Istým problémom môže byť aj obmedzená možnosť redundantnej konfigurácie, aj keď táto je možná. Je však potrebné zmeniť konfiguráciu databázového serveru, aby údaje replikoval a taktiež je nevyhnutné zdvojiť úložisko RRD súborov. Toto môže byť dosiahnuté replikáciou na úrovni blokového zariadenia alebo nasadením distribuovaného súborového systému. Samozrejme je možné nasadiť aj dve úplne nezávislé, ale identické inštalácie, no takéto riešenie má nevýhodu v zvýšenej záťaži monitorovaných zariadení a väčšom množstve prenesených údajov, nakoľko je potrebné rovnaké monitorovacie informácie prenášať dvakrát.

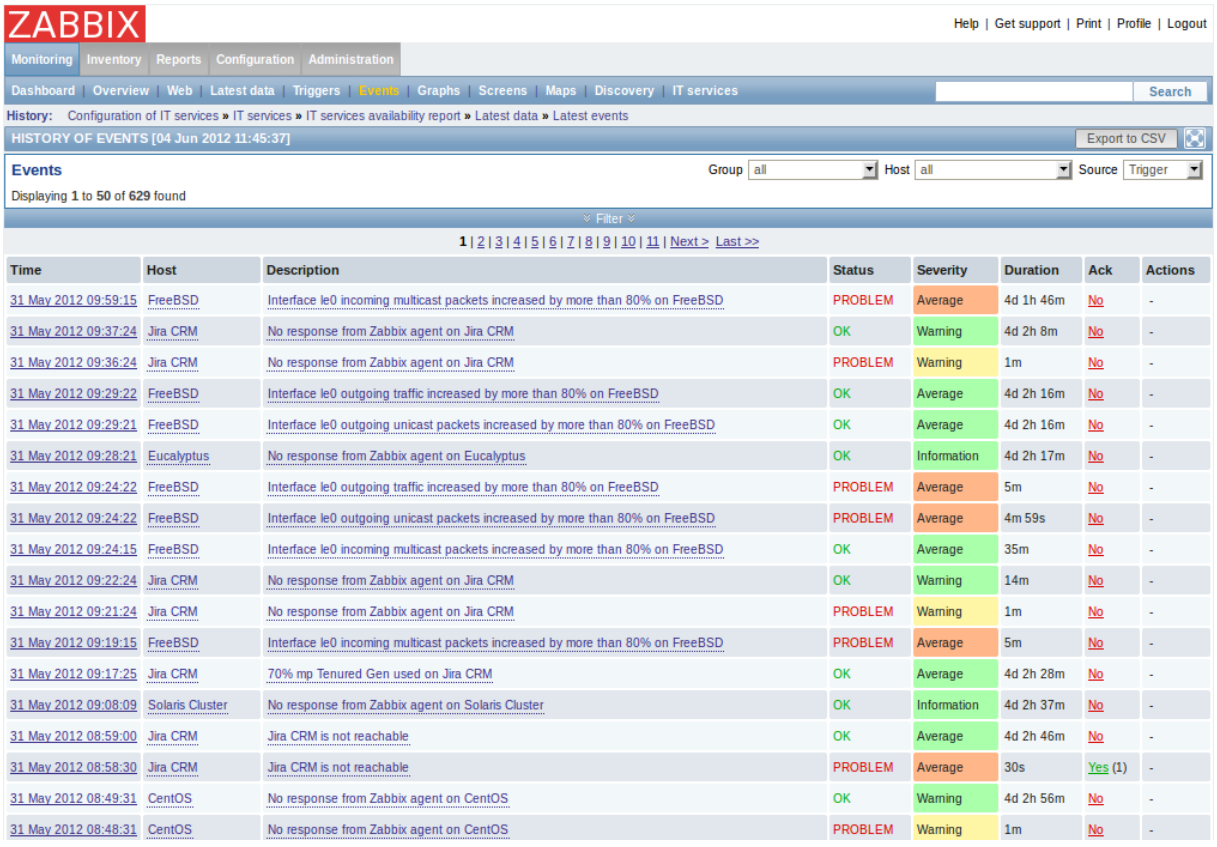
6. Alternatíva 2 – Zabbix

Inou možnosťou pre manažment siete Ústavu je využitie systému Zabbix. Ten je, podobne ako Cacti, napísaný v jazyku PHP (zobrazovacia časť) a jazyku C (server a agenty). Poskytuje enterprise-grade riešenie a pri tom je kompletné dostupný pod Open Source licenciou. To ho robí veľmi zaujímavým pre naše riešenie. Podobne ako Cacti umožňuje monitorovanie zariadení v sieti a rôznych veličín s vykresľovaním prehľadných grafických výstupov, filtrovanie, zaznamenávanie a spracovávanie chybových stavov a tvorbu dlhodobých štatistík.

Obr. 6: Zabbix - grafické znázornenie veličiny

Na získavanie údajov dokáže použiť protokoly SNMP, SSH, telnet, IPMI a JMX, ako aj TCP a ICMP. Taktiež má vlastného agenta pre rôzne operačné systémy. Ako databázu podporuje MySQL, PostgreSQL, SQlite, Oracle a IBM DB2. To z neho robí veľmi flexibilný nástroj vhodný do rôznych sieťových prostredí. V prípade poruchových stavov dokáže administrátora upozorniť rôznymi spsobmi, najmä e-mailom, SMS správou, alebo správou cez XMPP.

Zabbix vyžaduje oproti Cacti vyššie nároky na správu a údržbu, nakoľko je omnoho komplexnejší. Na druhej strane sú jeho funkcie viac centralizované a nevyžaduje, aby sme na splnenie požiadaviek inštalovali prídavné moduly. Taktiež má lepšie možnosti redundantnej konfigurácie a umožňuje dobrú integráciu so systémami na manažment konfigurácie, ako napríklad Puppet, cfengine, Chef alebo bcfg2 (žiadny takýto systém sme v našom návrhu nezahrnuli najmä pre pomerne malú veľkosť siete a tiež z dôvodu čiastočného vyriešenia tohto problému cez možnosti, ktoré ponúka Samba a Windows v súčasnosti).



Obr. 7: Zabbix - prehľad chybových udalostí

7. Možnosť koexistencie oboch alternatív

Vynára sa prirodzená otázka, či je možné uvedené riešenia použiť aj súčasne. V zásade tomu nič nebráni, dokonca je možné využiť rovnaký hardware. Bolo by však dobré optimalizovať získavanie údajov zo zariadení tak, aby nedochádzalo k duplicitnému prenosu, čo by malo za následok zvýšenú záťaž týchto monitorovaných zariadení a vyššie nároky na množstvo prenesených údajov.

Keďže však Cacti je v podstate podmnožinou funkcionality systému Zabbix, použitie obidvoch riešení nemá prakticky žiadny prínos. Práve naopak, prináša nevýhody v podobe vyšších nárokov na údržbu a systémové prostriedky.

8. Záver

V tejto práci boli analyzované možnosti manažmentu pre dohľad nad sieťou Ústavu telekomunikácií FEI STU. Na začiatku boli stanovené požiadavky, ktoré by mal takýto systém spĺňať, na základe nich boli následne navrhnuté dve alternatívne riešenia. Obidve pozostávali z aktuálneho stavu konfigurácie (centralizovaná správa používateľských účtov, dátové úložisko, ...), ktorý rozširujú o špecifickú aplikáciu zaisťujúcu monitorovanie a správu alarmov. Prvá z nich, odľahčená, s menšími nárokmi ale aj menšou funkcionalitou, navrhuje používať software Cacti. Druhá využíva možnosti monitorovacieho softwaru Zabbix, ktorý je omnoho komplexnejší. Tieto alternatívy dokážu fungovať aj súčasne.

Zdroje a použitá literatúra

[1] ISO/IEC, Information technology - Open Systems Interconnection - Systems management overview, ISO/IEC, 1998.

[2] „Rozdelenie IP sieti v ramci FEI,“ [Online]. Available: http://aladin.elf.stuba.sk/~emil/admin/ipnum.html.

[3] „Ústav Telekomunikácií FEI STU,“ [Online]. Available: http://www.ut.fei.stuba.sk/portal/?a=15&s=people.

[4] „Net-SNMP,“ [Online]. Available: http://www.net-snmp.org/. [Cit. 9 12 2012].

[5] „MySQL,“ [Online]. Available: http://www.mysql.com.

[6] T. Oetiker, „RRDtool,“ [Online]. Available: http://oss.oetiker.ch/rrdtool/.